UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF MISSOURI
EASTERN DIVISION

| | | |
|---|---|---|
| UNITED STATES OF AMERICA, | ) | |
| | ) | |
| Plaintiff, | ) | |
| | ) | |
| v. | ) | No. 4:02CR82 CDP |
| | ) | |
| GREGORY STRAUSER, | ) | |
| | ) | |
| Defendant. | ) | |

**MEMORANDUM AND ORDER**

This child pornography case is one of a number of cases arising from the government's investigation of the "Candyman" web site. The evidence against defendant Gregory Strauser was seized pursuant to a search warrant. The government concedes that the warrant affidavit falsely indicated that Strauser had received emails containing over one hundred images of child pornography, when in fact, there was no evidence that he had ever received any child pornography.

I previously held that Strauser had failed to show that the false information was knowingly or recklessly included, and so I denied his suppression motions. After additional evidence was discovered, I agreed to reconsider that decision. I now hold that the false information was recklessly included in the search warrant application, and that without the false information the warrant lacks probable cause, so I will grant Strauser's motion to suppress.

## Procedural Background

Defendant Gregory Strauser is charged with six counts of possession of child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B) and one count of using an interactive computer service for interstate transmittal of prohibited materials in violation of 18 U.S.C. § 1462. These charges all arose out of evidence obtained when law enforcement officers conducted a search of Strauser's home and computer pursuant to a search warrant on January 17, 2002.

All pretrial motions were referred to United States Magistrate Judge Audrey G. Fleissig pursuant to 28 U.S.C. § 636(b). Judge Fleissig held an evidentiary hearing on July 16 and 17, 2002, and entered extensive findings based on the evidence presented to her. She recommended that all of defendant's motions be denied. By order dated September 3, 2003 I adopted her factual findings in their entirety, and also followed her recommendation that the motions to suppress be denied. I agreed that the false information contained in the warrant application was included inadvertently and not intentionally or recklessly. Under Franks the inclusion of false information in a warrant application does not lead to suppression where the law enforcement agents obtaining the warrant did not know of, and were not reckless in not knowing of, the falsity of the information provided. My only disagreement with Judge Fleissig's Report and Recommendation was that I

concluded that probable cause would be lacking to support the issuance of the warrant if the false information were excluded. Under Franks, however, this makes no difference, since I agreed that the false information was not knowingly or recklessly provided.

After I denied the suppression motions, Strauser entered a conditional plea of guilty, reserving his right to appeal the suppression issues. Before he was sentenced, however, the government discovered and revealed additional evidence relating to whether the false information in the search warrant was provided knowingly or recklessly. At Strauser's request, I allowed him to withdraw his conditional guilty plea and I agreed to reconsider the motion to suppress, in light of the newly-discovered evidence. I held a hearing on the issue on February 14, 2003.

## Factual Background

Houston FBI agent Geoff Binney, as part of his ongoing duties to investigate child sexual exploitation, was engaged in searching the internet for child pornography. On January 2, 2001, Binney discovered The Candyman eGroup, and subscribed to the site. Candyman was a free site, and only required provision of an email address to join. After he subscribed, Binney received back a confirming email and thereafter he automatically received all emails from the

group. Binney remained a subscriber to the group until it was shut down by Yahoo on February 6, 2001. During that approximately one month period, Binney received 105 images of child pornography.

After he joined the Candyman eGroup, Binney contacted Yahoo to ask for additional information.[1] He spoke with a paralegal, Lauren Guarnieri, who was unhelpful, and, since he was unable to learn much from her, served a grand jury subpoena. In response, he received a letter and a multi-page list of email addresses. He contacted Guarnieri again, who confirmed that the list showed those email addresses that had subscriptions to Candyman at the time it was shut down. Binney was later reassigned, and the investigation was taken over by FBI Agent Kristen Sheldon. Sheldon attempted some additional investigation, and obtained a large number of logs from Yahoo, which indicated the dates the members had joined the group. She also served additional subpoenas and orders on Yahoo, although she did not actually obtain any additional documents until after the Strauser search warrant had been issued and executed.

---

[1]Yahoo acquired eGroups from another company some time in 2000, and eventually, toward the end of January of 2001, Yahoo converted the format of the eGroups to its own format, known as Yahoo groups. Thus, after Binney signed on, but before Candyman was shut down, the Candyman eGroup became a Yahoo group. Much of the evidence at the first hearing attempted to sort out the confusion caused by all this happening at the same time, because there are crucial differences between the sign on pages for eGroups and Yahoo groups. How the Yahoo groups operated is largely irrelevant to the issues presented here, however, because Candyman was an eGroup when Binney signed up.

Based on the investigation by Binney and Sheldon, the FBI sought a search warrant for Strauser's residence. The warrant application was actually signed by St. Louis FBI Agent Ann Pancoast. It indicated that an email account registered to Strauser subscribed to the Candyman group on December 26, 2000 and was still a member on February 6, 2001 when the service was shut down, and that the same email account had one active and one previously deleted screen name that could be viewed as sexually suggestive, specifically "EZ2bhrdnla" and "EZ2bhrdnSTL." The warrant application contains information confirming that Strauser lived at the address to be searched and that the screen names were registered to him. The application also contains generic information about how collectors and distributors of child pornography use computers. Other than the fact that Strauser had subscribed to Candyman on December 26, 2000, and had not "unsubscribed" as of February 6, 2001, however, there was nothing to indicate that he was a "collector or distributor of child pornography."

The search warrant application described the Candyman eGroup and described Agent Binney's experience with it, including that he had received emails containing 105 images of child pornography during the time he was a member of the group. The warrant application also stated that to subscribe to the Candyman eGroup one had to send an email to the site, and that all subscribers automatically

received via email all postings made by other members of the group, as well as email notifications whenever another subscriber uploaded a file to the site. The government now concedes that this information is false, and we now know that members did not necessarily receive all the emails. In fact, the vast majority of Candyman subscribers, including defendant Strauser, had exercised the "no mail" option, where they did not receive emails, although, as members, they could go to the web site and view files and previously-posted emails containing child pornography. There was no evidence in the affidavit that Strauser had actually done so. Thus, the application falsely implied that Strauser necessarily had received, during January and the first few days of February 2001, over one hundred images of child pornography, when in fact, there was no evidence that he had ever received any child pornography.

**The Franks Standard**

Under Franks v. Delaware, 438 U.S.154 (1978), a search warrant will be held invalid only where two conditions are met: (1) the application contains a false statement that was knowingly and intentionally made, or was made with reckless disregard for the truth, and (2) the false information is necessary to establish probable cause. To determine recklessness the Eighth Circuit has adopted the standard of "reckless disregard for the truth" used in First Amendment

libel cases. United States v. Clapp, 46 F.3d 795, 800-01 (8th Cir. 1995). This is a tougher test than the objective "knew or should have known" standard used in tort and other cases:

> [W]e have declined to adopt a definition of "reckless disregard" that incorporates the "subjective" versus "objective" terminology and have instead explained that
>
> > the test for determining whether an affiant's statements were made with reckless disregard for the truth is not simply whether the affiant acknowledged that what he [or she] reported was true, but whether, viewing all of the evidence, the affiant must have entertained serious doubts as to the truth of his [or her] statements or had obvious reasons to doubt the accuracy of the information he [or she] reported.
>
> United States v. Clapp, 46 F.3d at 795, 801, n 6. (8th Cir. 1995), quoted in United States v. Johnson, 78 F.3d 1258, 1262 (8th Cir. 1996).

United States v. Schmitz, 181 F.3d 981, 986-87 (8th Cir. 1999).

**Facts Relating to Whether the Falsehood was Knowingly or Recklessly Made**

The Candyman site was hosted as an "eGroup," and the initial page that Binney found for the Candyman site appears on the form template for other eGroups. Agent Binney testified that he saw a reference to the Candyman site in a pornography newsletter, and he simply typed in the web address shown in that newsletter to find the site. He identified Government's Exhibit 7 as a print out of

the initial page he found. The page has the name "The Candyman" and states "Founded December 6, 2000." Under "description" it states:

> This group is for People who love kids.
> You can post any type of messages you like too or any type of pics and vids you like too.
>
> P.S. IF WE ALL WORK TOGETHER WE WILL HAVE THE BEST GROUP ON THE NET.

The page showed 1164 members, the "Category" was described as "Top: Adult: Image Galleries: Transgender: Members." As with other eGroup pages, there were various buttons, including one labeled "Subscribe." The page also listed the following under "Addresses:"

> Post message: TheCandyman@egroups.com
> Subscribe: TheCandyman-subscribe@egroups.com
> Unsubscribe: TheCandyman-unsubscribe@egroups.com
> List owner: TheCandyman-owner@egroups.com
> URL to this page: http://www.egroups.com/group/TheCandyman

Gov. Exh. 7.

Agent Binney has testified on numerous occasions that he signed up for the Candyman site by copying the address listed under "Subscribe" and then pasting that address onto an email, which he sent. He testified that he did not subscribe by clicking on the "subscribe" button from the eGroup page, nor did he explore the other buttons on the page. This testimony, and the fact that both Judge Fleissig

and I credited it, was essential to my initial Franks determination, because there are different consequences dependent on how one subscribes.

If Binney had in fact subscribed by sending an email to the address "TheCandyman-subscribe@egroups.com" then he would not be shown any email options, but instead would receive a confirming email and then would automatically receive all emails posted by members of the group, as well as automatic email notifications whenever a member of the group uploaded a file. If, however, Binney had subscribed by clicking on the "subscribe" button, he would then have been shown a page giving him three email options.

When one clicks on the "subscribe" button, a page appears that contained a section headed "Message Delivery." The three options under this section included:

"Send email messages to [the member's email address]"

"Send a daily digest of messages [to the member's email address]" or

"Don't send me email, I'll read the messages at the Web site."

To get past this screen the user had to then click on the "Join" button at the bottom of the page. The default was "Send email messages to . . ." so if the user had simply gotten to the page and clicked "Join" without doing anything else, he would receive all email messages, provided that the eGroups already had his email

address.

When Binney first testified in this case, Yahoo had told the government that it could not tell from its records how he had subscribed, despite the fact that Yahoo's logs showed that Binney had subscribed "via web," while the logs showed that others had subscribed "via email." After Strauser entered his conditional guilty plea, however, the government continued its investigation and Yahoo provided different information. Yahoo now states that the "via web" annotation on the logs regarding Binney mean that Binney signed up by clicking on the "subscribe" button, and that he therefore had to have seen – and clicked on – the page setting out the different email options, including the "no mail" option. The parties to my hearing stipulated that this would be Yahoo's testimony. They also introduced by agreement the FBI "Cyber Division Special Technologies And Application Section Cyber Operational Deployment Unit Technical Report." This report indicates that FBI agents traveled to Yahoo's headquarters in California and examined Yahoo's source code for the eGroup. The report concludes that the log entry showing Binney's subscription to the Candyman site was generated as a result of Binney's clicking a button on the subscription web page that displays the email delivery options. Thus, the current Yahoo testimony, as verified by the FBI Cyber Division's review of the source code, shows that Binney could not have

signed up in the way he has repeatedly testified, and shows that Binney must have seen the email option page when he signed up.

Binney signed up for several other eGroups and Yahoo Groups after he signed up for the Candyman group. According to the Yahoo records entered by stipulation, Binney signed up for seven other groups, but Candyman was the first. The records show that he subscribed to all "via web." For one group, the records show Binney attempted to send an email on February 2, 2001 at 11:59 a.m., but that email was rejected by the site (or "bounced") and that he then subscribe to that same site "via web" at 12:32 that same day, and that subscription was accepted.

The government argues that I should not credit Yahoo's testimony now because Yahoo was uncooperative during the initial investigation and because Yahoo has changed its story. I believe the Yahoo testimony, however. First, Yahoo's prior testimony is not clearly conflicting. Yahoo witness McGoff did say at the first hearing that she could not tell, from the notation "via web" versus "via email" whether the person had signed up through an email or through clicking the "subscribe" button, but she also said she was not an expert on this and that Mark Hull would know more. Mark Hull was not asked about it when he testified at that hearing, so his current testimony is not contradicted by any prior sworn testimony. At Judge Fleissig's hearing most of the testimony from the Yahoo witnesses

related not to what "via web" and "via email" meant, but to the differences between eGroups and Yahoo groups, and whether the email options page would have been shown if one signed up via email, as Binney claimed he had done. Rejecting Yahoo's statement of what the logs means would require me to find that Yahoo provided the FBI Cyber Division with falsified code for their examination. There is no evidence to support this conclusion, and I believe that the evidence overwhelmingly shows that Binney joined by clicking the "subscribe' button, and that he therefore must have seen the screen showing the email options.

Binney's testimony about why he joined through an email does not make much sense. He testified that he did so because the browser was set up for another undercover email address, and he wanted any emails to come back to his gobannon@usa.net email account, so he copied the address and then pasted it into the "to" section of an email from the gobannon@usa.net account. (7/17/02 hearing, Tr. p. 2-157). Yet when later asked "What email address were you using when you were surfing around, looking for the Candyman web site?" he answered, "Gobannon@usa.net." (7/17/02 hearing, Tr. p. 2-191). Since one does not necessarily need an email address to browse the web, and since he has said that the browser was set up for somebody else, he must mean by this that he, at some point, entered the "Gobannon@usa.net" email address into either the eGroups

registration site, or into the email options page.

The Candyman web site had to receive Binney's email address at some time. If Binney had actually joined via email, then that would have been one way to receive it, but since the technical evidence, as verified by the FBI Cyber Division, is that he did not do so, then Candyman had to get his email address some other way. If he had already registered for eGroups, then it would have been provided that way and would not have to be reentered, but he never testified to any registration process. Although he signed up for several other eGroups after Candyman, this was the first one he joined, and there is no evidence that eGroups had his address before he first found the Candyman site (although the testimony of McGoff and Hull indicates that he would not have to reenter his email address when he joined the later groups, since he was already a member of one eGroup, Candyman). The most logical conclusion is that when he clicked on the "subscribe" button on the first page, that led him to the page with the email options, and he then had to enter his email address on that page. This means that he could not have simply "clicked through" the page without reading it, because the site had to have his email address from somewhere, and there is no evidence it came from anywhere else. Even if he did not have to enter his email address on that page, he still had to see the page and click on it.

The page that Binney had to have seen clearly indicated that one option was "Don't send me email." Yet Binney has repeatedly testified that he believed all members automatically got all emails, as he stated in the search warrant affidavit. This statement was the key to the probable cause, yet Binney did next to nothing to verify it, and there was no reasonable basis for him to believe it. He testified before me that his basis for this statement was almost entirely his own experience:

> THE COURT: What did you rely on when you drafted the affidavit?
>
> THE WITNESS: Your Honor, almost exclusively my experience.
>
> THE COURT: And what else?
>
> THE WITNESS: To the extent that Ms. Guarnieri, the conversation I had with her, played any part in it, as I said, I don't recall ever saying – that's another thing I rely on that to the extent it didn't do anything to dissuade me. Almost exclusively my experience, when I drafted the affidavit.

(2/14/03 hearing; Tr. p. 130, l. 5 to l. 15). And in the conversation with Guarnieri, that "didn't do anything to dissuade" him, Binney did not actually attempt to verify or confirm his assumption. Instead, as he has testified on multiple occasions, although his concern was with the unexpectedly large number of members and the lack of membership start dates, he only asked in passing about people who had sent emails or uploaded files – that is, people who he already

knew were active members, and for whom he would have probable cause even if they did not receive emails. His question to Guarieri was whether those persons would have received the same emails he did, and she said yes, but this was a very brief conversation, Binney believed Guarieri was being evasive, and Binney testified he did not really rely on her statements. His testimony about this conversation is very precise, and has been entirely consistent:

> The only thing I would like to add to that, while she did not do anything to dissuade my understanding, I didn't put a whole lot of stock in what she was saying. I used my experience to draft the affidavit that went out. It was apparent to me that she was trying to get me off the phone. I bring up this conversation, and I brought it up in my affidavit, only to show that she didn't do anything to dissuade my belief.

2/14/03 hearing, Tr. 124, l. 21 to 125, l. 18; see also 7/17/02 hearing, Tr. p. 2-176 to p. 2-177; 2/14/03 hearing, Tr. p. 45, l. 12 to p. 46, l. 8.

Thus, although the government has argued that Binney confirmed the false statement that everyone who signed up got all emails through this conversation with Guarnieri, Binney has never testified to that. Instead, he has repeatedly testified that his assumption all along was that everyone got all emails because he got all emails, and that he essentially did nothing to verify this assumption. While he says that in the conversation where he was trying to find start dates for members, he, in a round-about way, stated his assumption, and Guarnieri, who was

otherwise being very uncooperative and dismissive, did nothing to dissuade him, this is far from attempting to confirm the important assumption. Binney recognized how important this issue was, as he explained several times that if people had not sent emails or made postings, he had no probable cause absent the assumption that they had received the same emails he had received. But he never asked Guarnieri or anyone else at Yahoo whether that was true. And if he had read the screen that he saw when he signed up, he would have known that it was not true. And, seven more times before the search warrant was sought he signed up the same way, and so he had to have seen the same screen seven more times.

Although I continue to find from the evidence that defendant has not proven that Binney and Swenson knew that the information was false when they included it in the affidavits, I no longer find that their conduct was not reckless. In my prior order I stated that nothing indicated even negligence – that statement is clearly wrong, in light of the evidence that has now been provided. Binney and Swenson and the St. Louis agent who actually signed the affidavit[2] were all negligent in not making any efforts at all to verify that the "assumption" underlying the probable cause was valid. It is clear to me that Binney had no reasonable basis for

[2]The government has never argued that the warrant is valid merely because Agent Pancoast might not have known that the information provided by Binney was false.

believing that all subscribers to the site were receiving all email. In fact, the only information available to him contradicted this assumption: he had to click on a screen that required him to specify whether or not he wanted all emails, so it is clearly unreasonable to assume that everyone else had done what he did and asked to receive all emails. Indeed, based on what he knew about child pornographers, he should have considered it more likely that most subscribers would not have wanted all the emails to be automatically sent, out of concern that someone else, such as a family member or co-worker, might notice that the subscriber was receiving a high volume of emails. So, it is easy to find that the agents were negligent in including the false information, and it is easy to say that they had no reasonable basis for including the false information.

Under Franks, however, the standard is not whether the agent should have known more, or whether the agent should have investigated further, but whether the agent "entertained serious doubts as to the truth . . . or had obvious reasons to doubt the accuracy of the information." Schmitz, 181 F.3d at 987. Based on all the evidence before me, which I have extensively reviewed multiple times, I believe that defendant has met his Franks burden, and I find that Binney was reckless because he had obvious reasons to doubt the accuracy of the information he provided.

The government correctly points out that Franks issues cannot be viewed with the benefit of hindsight. See, e.g., United States v. Ozar, 50 F.3d 1440 (8th Cir. 1995). Indeed, some cases analyzing Franks appear to equate recklessness with a knowing falsehood, but close examination of the cases reveals that knowledge and recklessness remain two different things. Ozar stated, "Rarely will an unintentional omission be grounds for Franks v. Delaware relief when complex economic crimes are the subject of the investigation." 50 F.3d at 1445. This, however, is not a complex financial fraud case where even accountants could disagree over whether a crime had been committed. There is no doubt that possession of child pornography is a crime, and the only issue is a relatively simple one of whether evidence of that crime is likely to be found at a given location.

In United States v. Reinholz, 245 F.3d 765 (8th Cir. 2001), the Court of Appeals affirmed a finding of recklessness in a drug case. There the affidavit stated that a "confidential and reliable" informant had provided information that the target "is involved in the use of methamphetamine" and that the target "may also be involved in the manufacture of methamphetamine." In fact the informant was a pharmacist, who was no longer asking for confidentiality, and who had provided information that the target had legally purchased iodine crystals, which

the pharmacist believed had no legitimate use. Because the affidavit falsely implied that the informant had "personal knowledge of [the target's] methamphetamine use and distribution," when the officer knew the true facts, the court found recklessness. Similarly, in United States v. Gladney, 48 F.3d 309 (8th Cir. 1995), the court found recklessness by the affidavit's implication that the targets had been arrested at the scene of a prior seizure of money, when in fact they had been arrested in a different place at a different time. While both of these cases refused to suppress the evidence because the second prong of the Franks test was not met, they demonstrate that recklessness can be found in the absence of a knowing falsehood, and that the test is still that set out in Clapp: did the affiant entertain serious doubts or have obvious reasons to doubt the accuracy of the information?

I believe that the test is met here. The probable cause issue was quite simple: Is it likely that child pornography will be found? Binney repeatedly testified that he knew that without emails being received he did not have probable cause, except as to the people who had actually uploaded files or sent emails containing pornography. Yet even knowing this, he closed his eyes to obvious reasons to doubt his assumption. During this same time period, Binney had subscribed to seven other eGroups or Yahoo groups. Each time he subscribed "via

web," meaning that each time he was presented with the email options page and was required to click on that page to continue signing up. Yahoo had not been forthcoming and had not provided all the information that the FBI wanted, yet the FBI went forward with the false information in the warrant while it was still attempting to get more information from Yahoo.

In January of 2002, shortly after the warrant was executed, Yahoo produced (in response to the November 2001 requests) documents that showed on their faces that the vast majority of subscribers were of the "no mail" variety. Shortly after that, the originator of the Candyman site was arrested and told the FBI that most subscribers did not get email, but the FBI chose not to believe it. Although this was admittedly after the warrant was executed, the agents' reaction demonstrates their willingness to ignore obvious reasons to doubt their assumptions.[3]

The first prong of the Franks test has been met.

**Probable Cause**

The government has asked me to reconsider my previous ruling on the second prong of Franks – probable cause. I previously found that when the false

[3]Although I agree the agents' refusal to believe the truth lends support to the argument that their earlier behavior was reckless, I also believe it confirms that the falsehood was not knowing or intentional, since even when confronted with the truth both by the documents and by the person who should have known the most about the site, the agents refused to even consider that their unfounded assumption had been wrong.

information is excluded from the application, probable cause is lacking. I have reconsidered all of the issues and arguments, but continue to believe that absent the false information, the warrant application lacks a basis for finding probable cause to believe that child pornography would be found at Strauser's house.

If the false information contained in the affidavit is set aside, the only information regarding Strauser is that an email account registered to him subscribed to Candyman on December 26, 2000, and was still a member on February 6, 2001, when the site was shut down, and that the same email account had one active and one previously deleted screen name that could be viewed as sexually suggestive, specifically "EZ2bhrdnla" and "EZ2bhrdnSTL." Although the application contained generic information about how collectors and distributors of child pornography use computers, there was nothing other than the Candyman subscription to indicate that Strauser was a "collector or distributor of child pornography."

The warrant application contains significant information about the Candyman group, and there is no doubt that its reason for existence was the exchange of child pornography. Persons subscribing to the group would have to be aware of this once they had subscribed. The evidence also shows, however, and Agent Binney testified, that one could not be sure that the site contained child

pornography until after one had subscribed.

The government argues that only persons interested in child pornography would have subscribed to the service, and that if people who were not interested had subscribed accidentally, they could simply "unsubscribe," and then would not be listed as members when the site was closed down. The government argues that the warrant application contained sufficient information about collectors and distributors of child pornography and the use of computers to support a finding of probable cause. The argument is this: (1) only persons interested in child pornography would subscribe and not "unsubscribe," and (2) such persons should be equated with the "collectors and distributors" of child pornography described in the application, and (3) such persons are likely to have actually received child pornography from Candyman and have kept it.

I do not believe that these conclusions can legitimately be made from the evidence in the warrant. Essentially the government asks me to find that if a person one time subscribes to a service, whose content could not be known for sure until after subscribing, and the person never goes to the trouble of "unsubscribing," then that person is likely to possess child pornography. This is the equivalent of saying if someone subscribes to a drug legalization organization or newsletter, then there is probable cause to believe that person possesses drugs.

Yet I have never heard of the government requesting a warrant to search a home for drugs on such hypothetical evidence. In drug cases the government knows it must at least have some evidence of a delivery. Just as a warrant to search for drugs needs some evidence that there has been a delivery of drugs, a warrant to search for child pornography needs some evidence that there has been a delivery of child pornography.

The government counters that child pornography is different, because it can be delivered to one's home over the internet, without someone physically carrying it through the door. This argument confuses the mode of delivery with the fact of delivery. Yes, drugs or other contraband must be physically delivered from one location to another. Child pornography either can also be physically delivered, or an electronic image can be delivered over the internet. But for a finding of probable cause there must be some reason to believe that some contraband has been delivered at some time, by some means, whether one is authorizing a search for child pornography, for drugs, or for any other evidence of a crime. Saying that illegal items could be delivered over the internet is like saying that drugs could be delivered to a home when law enforcement was not watching, but we do not normally issue search warrants on this kind of speculation.

Here, a person could have clicked on the subscribe button, still not knowing

what was on the site, specified the "no mail" option, and then clicked on the "join" button. This hypothetical person could then have seen the child pornography on the site, been shocked, and immediately left the site, never to return, not even to search for and find the method of "unsubscribing." In such a case there would not be any emails containing child pornography sent, and the person would not receive or be in possession of any child pornography. Yet under the government's theory, probable cause would exist to obtain a warrant to search this person's home. I believe that the Fourth Amendment's requirement that "no Warrants shall issue, but upon probable cause" requires more.

Accordingly,

**IT IS HEREBY ORDERED** that the defendant's renewed motion to suppress evidence is granted.

**IT IS FURTHER ORDERED** that I will hold a telephone status conference with counsel on Monday, March 17, 2003, at 9:30 a.m., to discuss the next steps necessary to resolve this case. The Court will place the conference call.

_/s/_____
CATHERINE D. PERRY
UNITED STATES DISTRICT JUDGE

Dated this 6th day of March, 2003.